Some aspects on the feasibility of satellite quantum key distribution

C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, P. Villoresi

Department of Information Engineering, University of Padova, Italy

E-mail: bonatocr@dei.unipd.it

Abstract. In this paper we address some aspects on the feasibility of satellite quantum communication which we believe are still not well understood. We focus on the techniques to get a high enough SNR (in particular in the uplink) and to implement a polarization-preserving channel...

1. Introduction

For the last decades, a strong research effort has been devoted to study how quantum effects may be employed to manipulate and transmit information, in what is called Quantum Information Processing [1, 2, 3]. These research activities lead to new information-processing protocols with no classical counterpart, like quantum key distribution [4, 5, 6], quantum teleportation [7] or quantum computing [8]. Quantum Key distribution, in particular, is on its way from research laboratories into the real world. Fiber and free-space links have been realized linking nodes at larger and larger distances [9, 10] with higher and higher key generation rates. Network structures have also been demonstrated recently, for example the DARPA network in Boston [5] and the SECOQC network in Vienna [11].

However, current fiber and free-space links cannot implement a real global-scale quantum key distribution system. Fiber links have the advantage that the photon transfer is scarcely affected by external conditions, like background light, weather or environmental obstructions. On the other hand the extension of fiber links beyond few hundred kilometers is problematic, due to attenuation and polarization-preservation issues. Terrestrial free-space links show some advantages: the atmosphere provides low absorption and is essentially non-birefringent, allowing almost unperturbed propagation of polarization states. On the other hand, the optical mode is not confined in a waveguide, so they are extremely sensitive to the external environment: objects interposed in the line of sight, beam distortion induced by atmospheric turbulence, bad weather conditions and aerosols.

A solution to this problem can be the use of Space and satellite technology. Space-based links can potentially lead to global-scale quantum networking since they allow

a much larger propagation distance of photonic qubits compared to present terrestrial links. This is mainly due to the fact that most of the propagation path is in empty space, with no absorption and turbulence-induced beam spreading, and only a small fraction of the path (corresponding to less than 10 km) is in atmosphere. However many technical problems must be overcome in order to realize a working quantum communication link between Earth and Space. Geostationary satellites are too distant to implement a single photon link, therefore fast-moving low-orbit satellites (LEO orbit, from 500 to 2000 km above Earth surface) must be employed.

Several proof-of-principle experiments in this direction have been performed recently. In 2005 C.-Z. Peng and coworkers reported the first distribution of entangled photon pairs over 13 km, beyond the effective thickness of the aerosphere [12]. This was a first significant step towards satellite-based global quantum communication, since it showed that entanglement can survive after propagating through the noisy atmosphere.

In 2007 two experiments were carried out at Canary islands by a European collaboration. Entanglement-based [10] and decoy-state [13] quantum key distribution was realized on a 144 km free-space path, linking La Palma with Tenerife. For these experiments the Optical Ground Station of the European Space Agency, developed for standard optical communication between satellites and Earth, was adapted for quantum communication. It is important to highlight that the twin-photon source was able to achieve coincidence production rates and entanglement visibility sufficient to bridge the attenuation expected for satellite-to-ground quantum channels.

In a successive experiment, the feasibility of single-photon exchange for a down-link between a LEO satellite and an optical ground station (Matera Laser Ranging Observatory, in the South of Italy) was experimentally demonstrated [14]. The researchers exploited the retroreflection of a weak laser pulse from a geodetic satellite covered with corner-cubes (Ajisai, orbiting at around 1400 km) to simulate a single photon source on a satellite. They showed that, implementing a strong filtering in the spatial, spectral and temporal domain the emitted photons can be recognized against a very strong background.

In this paper, we present a detailed analysis of the feasibility of satellite-based quantum communication which we believe have not yet been adequately discussed in the literature. In particular, we concentrate on two issues that were identified as crucial by the experiment performed at Matera Observatory [14]: the possibility of a good signal-to-noise ratio (SNR) and the polarization mainteinance in the link. As regards the SNR we will refine the models already presented in the literature by introducing a detailed analysis of the effect of atmospheric turbulence and of the background stray-light in the case of a ground-to-satellite uplink. We will then discuss some filtering techniques to improve the SNR reducing the noise level; in particular we will analyse in detail the possibility of high-accuracy temporal filtering. Finally, as long as polarization control is concerned, we will discuss and compare different strategies to implement a polarization-conserving channel.

2. Signal and Noise

Two crucial points for any communication system are the amount of attenuation of the link and the noise introduced in the system. This is even more important for quantum communication since the signal transmitted by Alice is ideally one photon (or a weak coherent pulse with very low mean photon number in many realistic implementations). Therefore one cannot increase the signal power in order to have a good enough SNR: the only available tools are the reduction of the link attenuation and of the background noise. In this section we will analyze a quantum channel between a ground station and a LEO satellite both in the uplink and the downlink, presenting a model for the expected attenuation and background noise.

2.1. Signal attenuation

The main factor limiting the performance of free-space optical communication is atmospheric turbulence, both for terrestrial horizontal links or for links between ground and satellites. Atmospheric turbulence induces refractive index inhomogeneities, that increase the amount of spreading for traveling beams [15]. In particular, turbulent eddies whose size is large compared to the size of the beam induce a deflection of the beam (beam wandering), while smaller-scale turbulent features induce beam broadening. In other words, observing a beam which propagates through turbulent atmosphere at different time instants, one can see a broadened beam randomly deflected in different directions. When integrating the observation over a time-scale longer than the beam-wandering characteristic time, the global effect is a large broadening of the beam.

Models for optical beam propagation in the case of uplinks and downlinks between a satellite and a ground station have been discussed in the literature [16, 17, 18]. In the case of a Gaussian beam of waist w_0 and intensity I_0, the average long-term spot (which is a superposition of moving short-term spots), tends theoretically to a Gaussian spatial distribution of intensity [17]:

$$\langle I(r,L)\rangle = I_0 e^{-2r^2/w_{LT}^2} \tag{1}$$

with width w_{LT}, where

$$w_{LT}^2 = w_{ST}^2 + 2\left\langle \beta^2 \right\rangle \tag{2}$$

Here w_{ST} is the short-term beam width, while β is the instantaneous beam displacement from the unperturbed position.

It can be shown that, for a collimated beam, the long-term beam width is [17]:

$$w_{LT}^2 = w_0^2\left(1+\frac{L^2}{Z_0^2}\right) + 2\left(\frac{4L}{kr_0}\right)^2 \tag{3}$$

where Z_0 is the Rayleigh parameter of the beam, L is the propagation distance and r_0 is the Fried parameter, given by:

$$r_0 = \left[0.42k^2\int_0^L C_n^2(z)\left(\frac{L-z}{L}\right)^{5/3} dz\right]^{-3/5} \tag{4}$$

The estimate of r0 in equation (4) was made by integrating the turbulent contribution of the atmosphere along the whole optical path. The resulting w_{LT} should then be considered a high bound, and the resulting conclusions as on the safe side. The refractive index structure constant $C_n^2(z)$ is taken from Ref. [16] to be:

$$C_n^2(h) = 0.00594(v/27)^2(h\cdot 10^{-5})^{10}\cdot e^{-h/1000} + 2.7\cdot 10^{-16} e^{-h/1500} + A\cdot e^{-h/100} \quad (5)$$

where $A = 1.7 \cdot 10^{-14}$ and $v = 21m/s$. The expression for the short-term width is:

$$w_{ST}^2 = w_0^2 \left(1 + \frac{L^2}{Z_0^2}\right) + 2\left\{\frac{4.2L}{kr_0}\left[1 - 0.26\left(\frac{r_0}{w_0}\right)^{1/3}\right]\right\}^2 \quad (6)$$

The receiving telescope can be described as a circular aperture of radius R, which collects part of the incoming beam and focuses it on a bucket single-photon detector. The power P received through a circular aperture of radius R centered on the beam is:

$$P = 2\pi I_0 \int_0^R \rho e^{-2\frac{\rho^2}{w_{LT}^2}} d\rho \quad (7)$$

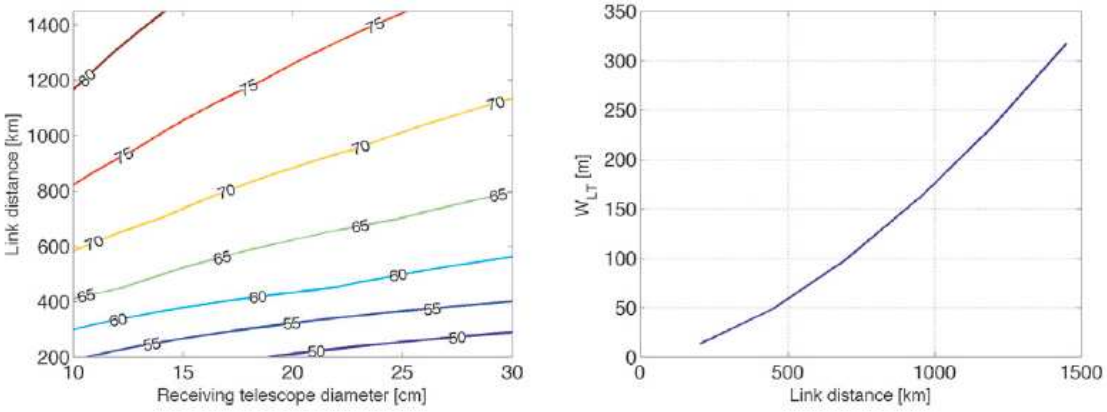


Figure 1. Attenuation η of the link (dB) as a function of the link distance and receiver telescope diameter for the long-term beam spreading effect, which takes into account the effects of beam spreading and wandering. The operating wavelength is $\lambda = 800nm$ and the diameter of the Earth-based transmitting telescope is assumed to be 1.5 m. On the right-side a zoom of the figure on the left for the link distance between 200 and 500 km.

Therefore the link-efficiency η, which we define as the percentage of the received power with respect to the transmitted one is:

$$\eta = \eta_0 \left(1 - e^{-\frac{2R^2}{w_{LT}^2}}\right) \quad (8)$$

The factor η_0 comprises the detection efficiency, the pointing losses and the atmospheric attenuation; we take an empirical factor [19] $\eta_0 \approx 0.1$.

Some simulations for the link efficiency are shown in Fig. 1: the link attenuation (in decibels) is shown as a function of the link distance L and the radius R of the receiving telescope. In the uplink the beam first travels through the turbulent atmosphere and

then propagates, aberrated, in the vacuum to the satellite. The initial atmosphere-induced aberrations greatly increase the beam spreading, resulting in a very strong attenuation. For a relatively low satellite, at 500 km above the Earth surface, the attenuation is on the order of more than 50 dB.

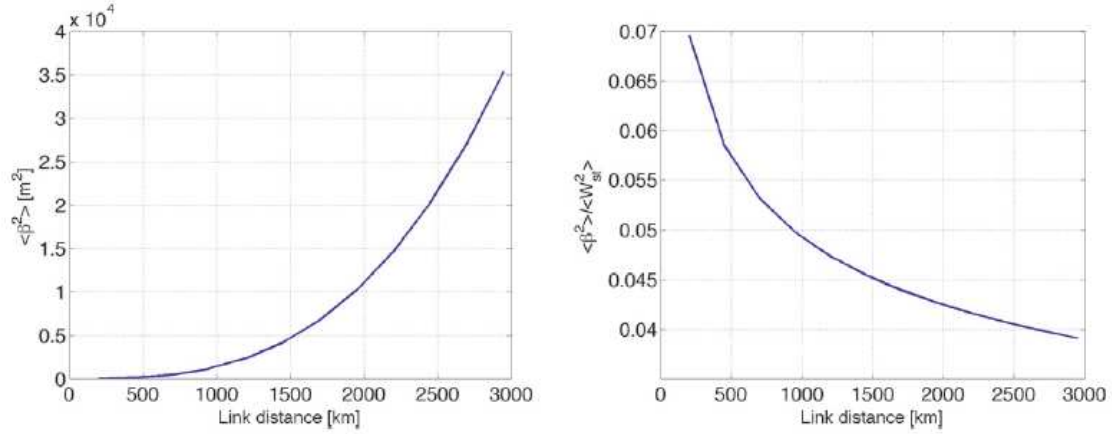


Figure 2. On the left, $\langle \beta^2 \rangle$ as a function of the ground-to-satellite distance. On the right, ratio between $\langle \beta^2 \rangle$ and $\langle w_{ST}^2 \rangle$. In the case of a LEO satellite, the effect of beam wandering is clearly limited to less than 10 percent with respect to the beam spreading; therefore its possible compensation with a tip/tilt active system might not significantly improve overall performance of the link.

An interesting point is the relative contribution of the beam spreading due to smaller-scale atmospheric turbulence (described by w_{ST}) and the the beam-wandering induced by larger-scale eddies (described by $\langle \beta^2 \rangle$). In principle the beam wandering could be compensated by means of an active tip/tilt mirror with some kind of feedback loop. However, as it is shown in Fig. 2, the benefit that one could get is below 10 percent, making such compensation practically worthless.

2.2. Noise

2.2.1. Up-link (day-time operation) During the day the main source of background noise is the sunlight reflected by the Earth surface into the telescope field of view (see Fig. 3). Let H_{sun} be the solar spectral irradiance (photons/ $s\ nm\ m^2$) at one astronomical unit and a_E the Earth albedo; assuming a Lambertian diffusion, for which the radiance is independent of the angle, the spectral radiant intensity reflected by the Earth (number of photons per s, nm and sr) is:

$$S_E = \frac{1}{\pi} a H_{sun} \Sigma \tag{9}$$

where Σ is the emitting area seen by the telescope and $H_{sun} = 4.61 \cdot 10^{18}$ photons/ ($s\ nm\ m^2$) at $\lambda = 900$ nm. Such photons are collected by an optical system having entrance

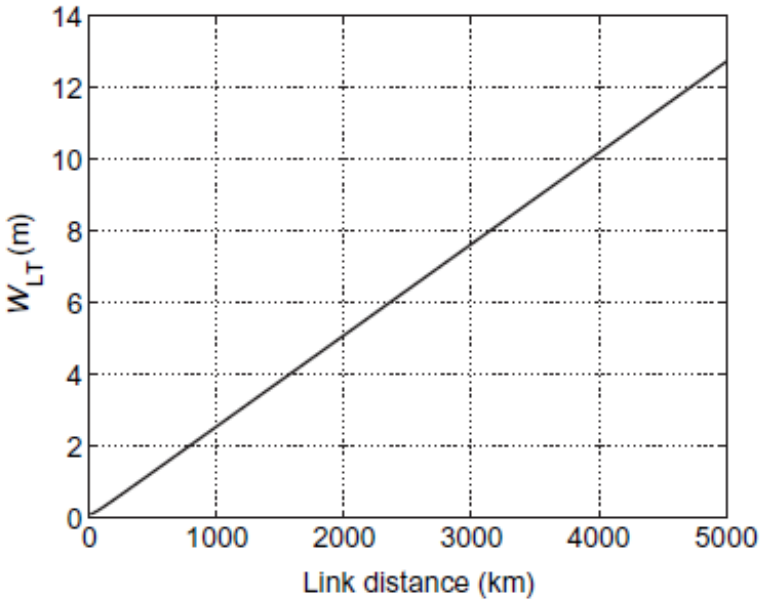


Figure 3. Scheme to calculate the background noise in the uplink. Sun (or Moon) light is reflected by the Earth surface (with Lambertian diffusion) into the receiving telescope field-of-view.

aperture raius r and instantaneous field-of-view $IFOV$, at distance L from the Earth surface. Therefore the emitting area is:

$$\Sigma = (\text{IFOV})^2 L^2 \tag{10}$$

and the solid angle from which the telescope on the satellite can be seen from Earth is:

$$\Omega = \frac{\pi r^2}{L^2} \tag{11}$$

Therefore the number of background photons collected by the optical system per units of $\Delta\nu$ and Δt is:

$$N_{day} = \frac{1}{\pi} a_E H_{sun} \Sigma\Omega = a_E r^2 (IFOV)^2 H_{sun} \tag{12}$$

2.2.2. Uplink (night-time operation) The dominant sources of background radiation from the Earth surface during night are its black-body emission and the reflected moon light. In realistic situations there will be a significant contribution of scattered light from human activities, which depends on the specific location considered.
The number of photons per ($s\ nm\ m^2$) emitted by a black body, according to Planck's law, is:

$$S_{bb} = \frac{2c}{\lambda^4} \frac{1}{e^{\frac{hc}{\lambda kT}} - 1} \tag{13}$$

At $T = 293$ K and $\lambda = 800$ nm, $S_{bb} = 3.1 \cdot 10^6$ photons per ($s\ nm\ m^2$).

Let's now calculate the radiance due to moonlight reflection on the Earth. Given the solar spectral irradiance H_{sun}, the number of photons per s and nm which hit the

Moon surface is: $H_{sun} \cdot \pi R_M^2$ where R_M is the Moon radius. Assuming Lambertian diffusion, the number of photons per ($s\ nm\ sr$) reflected by the Moon is:

$$\tilde{P}_{moon} = \frac{a_M}{\pi} S_{sun} \pi R_M^2 \tag{14}$$

where a_M is the Moon albedo. Assuming the Moon at normal incidence, the solid angle to the area on Earth Σ seen by the telescope is:

$$\Omega_\Sigma = \frac{\Sigma}{d_{EM}^2} \tag{15}$$

where d_{EM} is the distance Earth-Moon. The spectral radiant intensity after Lambertian reflection from the Earth surface is:

$$S_E^{(M)} = \frac{1}{\pi} a_E a_M S R_M^2 \frac{\Sigma}{d_{EM}^2} \tag{16}$$

The number of photons per second and nm of bandwidth entering the receiving telescope (radius r, field-of-view $IFOV$) is:

$$N_{night} = \alpha N_{day} \tag{17}$$

where:

$$\alpha = a_M \left(\frac{R_M}{d_{EM}} \right)^2 \tag{18}$$

is the ratio between the background radiance at night-time (full Moon) and day-time. Assuming the Moon albedo to be $a_M \approx 0.12$ we have that α is of the order of 10^{-6}: during night-time, in full Moon conditions, we have approximately a reduction of six orders of magnitude in the amount of background noise.

2.3. Down-link

2.3.1. Signal attenuation and turbulence The effect of the atmospheric turbulence on a plane wavefront is a phenomenon very relevant to the FOV limit in the noise reduction of a quantum channel, as seen above. In particular, the predominance of broadening of the beam or of the rapid bending of the beam, described by the long- and short-terms in the far-field width is a crucial information in order to design the optical system aimed at the mitigation of the turbulence effects.

To this purpose, experimental data taken by means of a ground telescope are suitable to be compared to the modeling presented before. In our experiment we have acquired with a video recorder the flickering light from Vega (α-Lyrae, magnitude=0) by the Matera Laser Ranging Observatory of Agenzia Spaziale Italiana in Matera, Italy. The telescope has the primary mirror diameter of 1.5 m. The gathered light was spectrally filtered in the green by the coated optical components of the CoudÃ¨ path, and acquired on the focal plane by a bidimensioanl sensor whose square pixel size was of 6.7 μm. The collection of the frames were analyzed in order to extrac the first two moments of the intensity distribution. The results is reported in the Figs .. ..

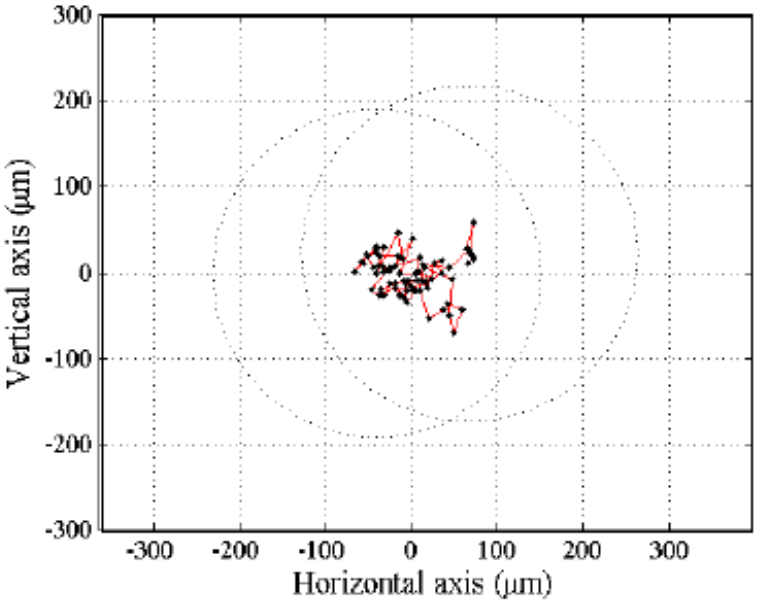


Figure 4. Number of photons at day-time (left side) and night-time (right side) as function of telescope IFOV where $\Delta\nu = 1nm$, $\Delta t = 1ns$. The number of background photons entering the telescope during night-time in full-Moon conditions is approximately six order magnitude larger than the value for day-time operation.

2.3.2. Background light noise The background noise for a satellite-to-ground link was examined in details by Miao et al. [20]. The noise power P_b received by a ground-based telescope pointing a satellite in the sky can be expressed as:

$$P_b = H_b \cdot \Omega_{fov} \cdot \pi r^2 \cdot \Delta\nu \tag{19}$$

where H_b is the brightness of the sky background in $W\ m^{-2}\ sr^{-1}\ \mu m^{-1}$, Ω_{fov} the field of view of the telescope in sr and r its radius; $\Delta\nu$ is the filter bandwidth. H_b is strongly related to the weather conditions, for example during.

We calculated the signal-to-noise ratio for the downlink using our results for the signal attenuation in a turbulent atmosphere and the noise parameters given in [20]. The results are shown in Fig. 6. On the left side, the down-link attenuation is shown as a function of the link distance L and the radius of the Earth-based receiving telescope. Two factors result in an increased performance for the downlink with respect to the uplink. First, on Earth we can have larger receiving telescopes than in space. Second, the beam first propagates in the vacuum with just diffraction spreading and gets in contact with the turbulent atmosphere only in the final stage of propagation. Therefore the aberrations introduced by turbulence only affect weakly the wavefront before it enters the telescope.

On the right side of Fig. 6 we plotted the SNR as a function of the sky brightness ($\Delta\nu = 1$ nm, $IFOV$). The SNR is greater than one only at night-time.

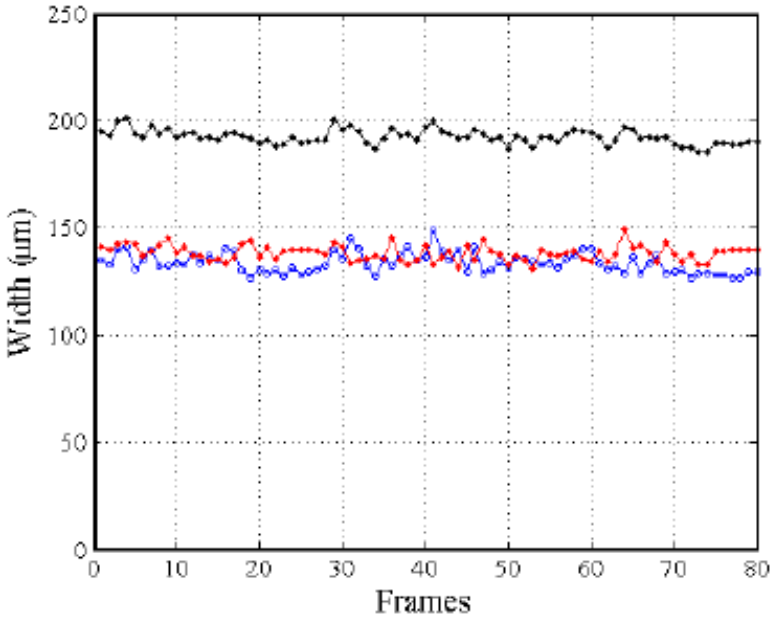


Figure 5. Signal-to-noise ratio (in dB) at day-time (left side) and night-time (right side) as a function of telescope IFOV and satellite distance. The curves on the left sign correspond to negative values for the SNR in decibels; this means that the SNR is lower than 1, clearly to low to establish a quantum communication link. On the other hand, SNR as high as 100:1 or 1000:1 can be envisaged during night-time. The operating wavelength is $\lambda = 800$ nm and the transmitting telescope diameter is 1.5 m. We assume a filtering bandwidth $\Delta\nu = 1$ nm and a gating time of $\Delta t = 1$ ns for the detectors.

2.4. Filtering and synchronization

As discussed in the previous sections, in order to have a significant signal-to-noise ratio to establish a quantum communication link, it is crucial to reduce the amount of noise. Moreover, the management of detector dead-time is also a crucial point. Avalanche single-photon detectors are characterized by a certain amount of time, after a detection event, in which they cannot detect any more photons. For single-photon avalanche photodiodes the dead time can vary from 40 to 100 ns. For this reason the detection of a noise photon has a double negative effect: it decreases the final secure key rate and it blinds the detector for the duration of the dead time preventing the detection of a good photon. This is why very often QKD systems run in gated-mode: the detectors are switched-on only when a signal photon is supposed to arrive. To allow the possibility to gate the detectors, high-accuracy temporal synchronization is mandatory.

Filtering strategies can be divided in three categories: spectral, spatial and temporal. Spectral filtering is pretty easy to implement even on a Space setting, just employing interference filters which must be thermally stabilized. Spatial filtering can be implemented acting on the receiving telescope field-of-view, in order to select only photons coming from the right directions. A trade-off must be found between the need

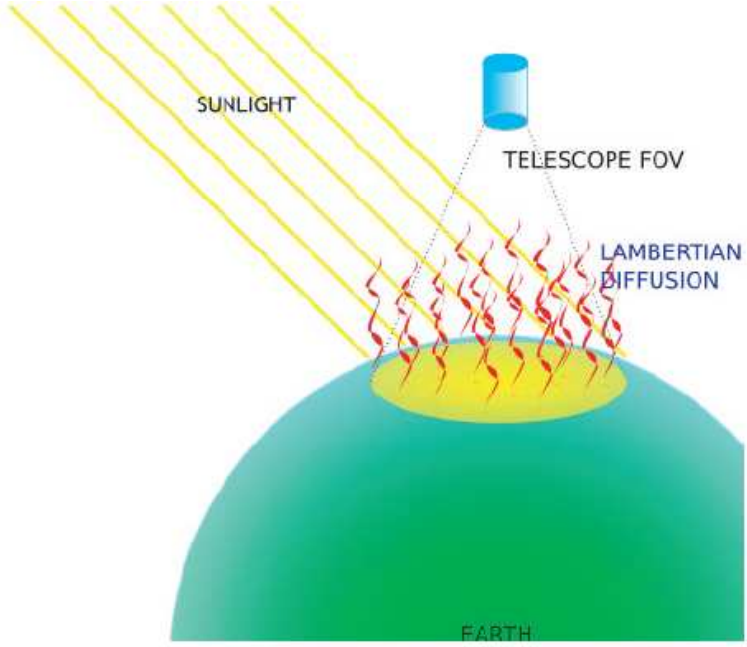


Figure 6. Simulations for the downlink. On the left side, link attenuation (in dB), as a function of the diameter of the satellite-based transmitting telescope and of the link distance L. On the right side, SNR of the link as a function of the sky background noise for different link distances, assuming a diameter of the transmitting telescope $r = 15$ cm. All simulations are performed assuming a diameter of the Earth-based receiving telescope $R_X = 1.5$ m, with field-of-view 0.016 degrees (corresponding to MLRO, Matera)

of a strong spatial selectivity (to have efficient noise-reduction) and the possibility of imperfect pointing, which would call for a relaxation in spatial filtering.

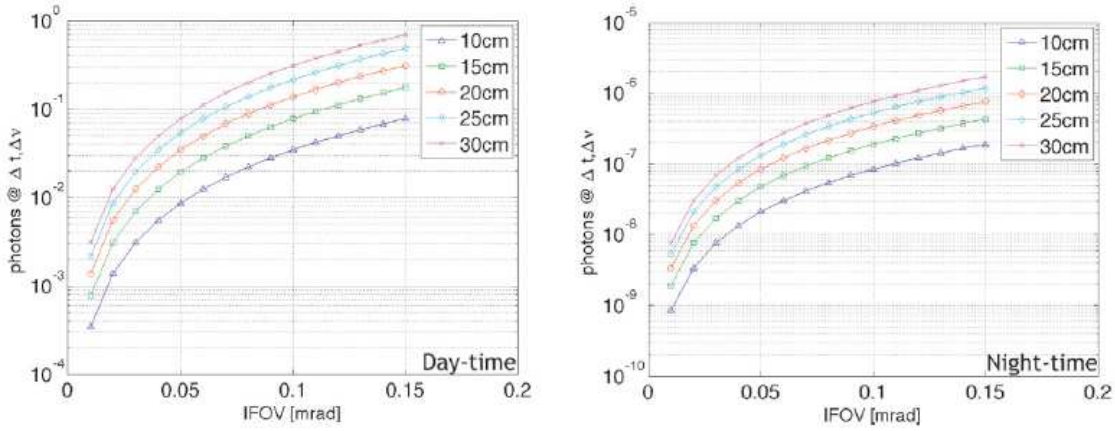


Figure 7. Data analysis of the KHz laser-ranging data of a typical passage of the GRACE satellite (altitude around 400 km). On the left side time derivative of the range time as a function of time, on the right-side histogram of the same quantity. The temporal variation of the range time is around $40\mu s/s$.

In a Space environment, time filtering is a more delicate issue, because it requires really good synchronization between two devices in fast relative motion. Such precise synchronization is fundamental in order to discriminate the good photons from the background noise and in order to have gated-mode operation of the detectors. For the latter, the arrival time of a signal photon need to be known in advance, in order to open the detector gate. Let's focus to the case of an Earth-based station sending photons to an orbiting receiver. Two different schemes have been used in the literature to synchronize free-space QKD systems: self-synchronization and external synchronization.

In the case of self-synchronization a periodic bright pulse of a wavelength different from the one of the signal photons can be used to open the detector gate. This technique was used, for example, in one of the seminal experiments about free-space QKD by Hughes and co-workers [21]. The waveform of the pulses can be shaped in order to code in the synchronization frames some information regarding the communication itself. A different option is to use an external synchronization technique, for example stabilized local clocks and software-controlled phase-lock loop driven by the detected photon signal (as described by Rarity et al. in [22]) or by the global positioning system (GPS) signal (as done R. Ursin and coworkers for entanglement distribution over 144 Km in free-space [10]). In the case of satellite-based quantum communication this technique requires the precise a priori knowledge of the orbit, which makes it extremely unpractical.

Here we will focus on the self-synchronization technique, which we believe is easier to realize in practice and gives the signal for the detector-gating control with no need to know precisely the station-satellite distance. An interesting question is then what repetition rate shall be imparted to the synchronization pulses in order to keep a control on the satellite position on the order of the tens of centimeters (which correspond to trip-times to the order of one nanosecond). In Fig. 7 we show some data analysis performed on KHz laser ranging data for the GRACE satellite acquired by the Graz Space Research Center. From the laser-ranging data we calculated the time derivative of the photon trip-time from ground to the satellite and we plotted it on a histogram. The results clearly show that the trip-time changes of the order of $40\mu s$ per second (which corresponds to about 12 Km per second). This means that if we want to keep track of the changes with an accuracy to the order of the nanosecond we need a repetition rate for the synchronization of the order of $50 - 100$ KHz.

3. Polarization Control

A second crucial point for the implementation of quantum communication schemes based on polarization-encoded qubits is, of course, the preservation of polarization states in the channel.

As it was shown in [23], propagation in the atmosphere does not affect significantly the polarization stets, nor does the Faraday effect due to the Earth magnetic field. The use of curved optics in an off-axis configuration introduces some spatially-dependent polarization effects [24] which can lead to global decoherence of the polarization-encoded

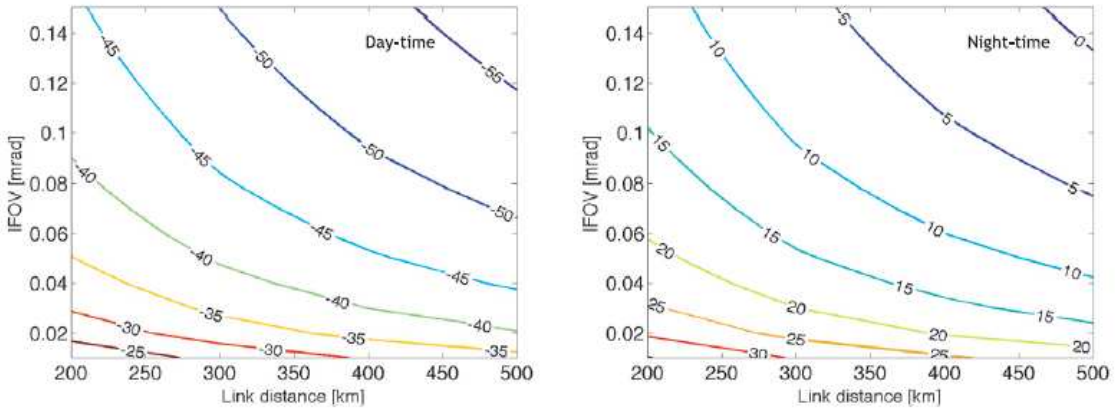


Figure 8. Scheme of the satellite tracking system and its effect on polarization, as discussed in [23]. A source on a satellite emits a stream of single photons, which are directed to ground by a moving pointing mirror. A second pointing mirror on ground receives the photons and whatever direction they come from, it sends them to the detection apparatus. Due to the relative motion between the satellite and the ground station, there is a relative rotation of the polarization axes and a change in the mirror incidence angles, which induces a time-dependent polarization transformation on the qubits.

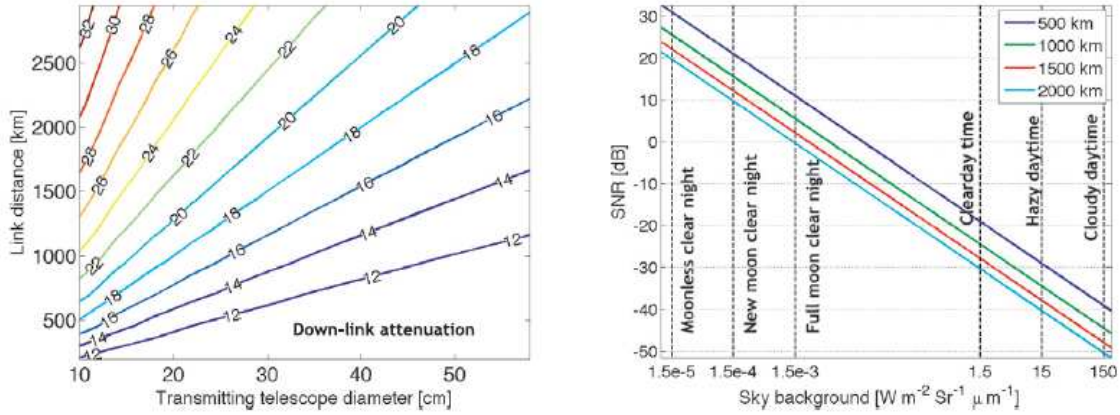


Figure 9. Example of temporal evolution of the Stokes parameters at the receiver for a fixed vertically-polarized state emitted on the satellite. In a few-minutes passage the values of the Stokes parameters change dramatically in a smooth way.

qubits. However, the effect is small for on-axis optics and it can be neglected, just having some care in the design of optical systems.

On the other hand, the relative motion of the satellite and the ground station induces a time-dependent transformation on the polarization state as seen by the receiver. This is mainly due to the relative rotation of the satellite vertical axis with respect to ground and change in the polarization induced by reflection on mirrors at time-varying angles. The effect, in the case of a single passage of a LEO satellite orbiting at 400 Km from the Earth surface, is shown in Fig. 9: given a photon which is emitted

with vertical-polarization in the satellite reference frame, the Stokes parameter seen by the ground-based receiver are plotted as a function of time.

If we can neglect channel depolarization effects, as it is the case for atmospheric propagation, polarization states can be represented by Jones vectors:

$$\begin{bmatrix} A \\ Be^{i\varphi} \end{bmatrix} \qquad A, B, \varphi \in R \quad A^2 + B^2 = 1 \tag{20}$$

The channel properties are described by a 2-by-2 time-dependent Jones matrix $C(t)$, which transforms the polarization states according to $J(t) = C(t)J_0$. To establish a successful quantum link based on polarization-encoded qubits, such transformation must be compensated. This can be done characterizing the channel without interfering with the single-photon exchange, in order to measure such matrix $C(t)$. Then, applying the inverse transformation $C^{-1}(t)$ for every time instant t to the incoming photons, the correct state can be restored before performing the measurements needed fro quantum key distribution.

However, in general, not to interfere with the signal photon exchange, the characterization of the channel Jones matrix is to be performed with different parameters than the photon exchange. For example, a different wavelength may be employed, or the two operations of channel-probing and quantum-communication can be performed at in different time-slots. Defining $C_P(t)$ as the experimentally measured channel Jones matrix, we have:

$$C_P^{-1}(t)C(t) = E(t) \tag{21}$$

with $E(t) \to I, \quad \forall t$ in the case of ideal compensation. Let $\{E_{ij}(t)\}, i, j = 1, 2$ be the elements of the matrix $E(t)$.

In this Section we will discuss some polarization-compensation schemes, discussing their effectiveness in the case of the model presented in [23]. Considering a BB84 quantum key distribution scheme, photons are transmitted in two non-orthogonal bases, for example the horizontal/vertical one (states $|H\rangle$ and $|V\rangle$) or the diagonal one (states linearly polarized at ± 45 degrees, that we will indicate respectively with $|+\rangle$ and $|-\rangle$ degrees). The average error probability is:

$$P_E = 1 - P_{HH} - P_{VV} - P_{++} - P_{--} \tag{22}$$

where P_{ij} is the temporal average of the conditional probability of measuring the state i once j has been transmitted ($P_{ij} = \langle p(r = i|t = j)\rangle$).

Suppose now to have a horizontally-polarized state transmitted at time t_i. After compensation, one gets the state:

$$J(t_i) = \begin{bmatrix} E_{11}(t_i) & E_{12}(t_i) \\ E_{21}(t_i) & E_{22}(t_i) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} E_{11}(t_i) \\ E_{21}(t_i) \end{bmatrix} \tag{23}$$

so that the probability of obtaining the correct result is $|E_{11}(t_i)|^2$. Assuming that the probability of transmitting a $|H\rangle$ state is $\frac{1}{4}$:

$$P_{HH} = \frac{1}{4} \left\langle |E_{11}|^2 \right\rangle \tag{24}$$

With similar arguments one can find expressions for the other conditional probabilities so that:

$$P_E = 1 - \frac{1}{8}\left\langle \left\{ 3|E_{11}|^2 + 3|E_{22}|^2 + |E_{21}|^2 + |E_{12}|^2 + E_{11}^* E_{22} + E_{11} E_{22}^* + E_{12}^* E_{21} + E_{12} E_{21}^* \right\} \right\rangle \quad (25$$

3.1. Probe beam at a different wavelength

One possible way of measuring the channel Jones matrix without perturbing the single-photon exchange is using a probe beam at a wavelength λ_p different from the one of the signal beam (λ_s). In this case the signal transformation Jones matrix is $C(\lambda_s)$, while the compensation matrix is $C(\lambda_p)$. Thefore:

$$E = C^{-1}(\lambda_p) C(\lambda_s) \quad (26)$$

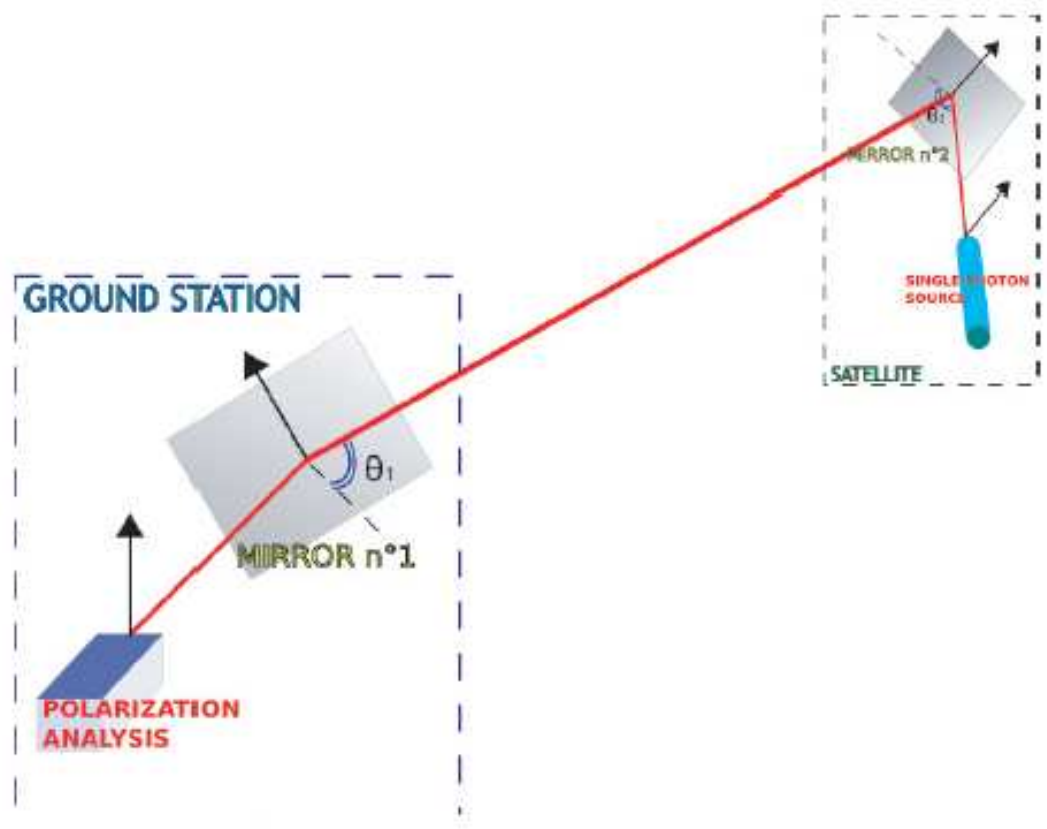


Figure 10. Polarization-state preservation in the satellite-based quantum channel, in the case of a channel-probing beam at a different wavelength with respect to the signal. The bit error rate due to imperfect compensation is negligible even for probing wavelengths quite far from the signal one ($\lambda_s = 800$ nm).

To have a statistical evaluation of the degree of compensation that can be achieved with this technique we performed a simulation for 1000 passages of a LEO satellite orbiting at 500 Km. We used the model described in [23] to calculate the matrices $C(\lambda_s)$ and $C(\lambda_p)$ for a uniform temporal sampling of each passage ($\Delta t = 1$ s). Then

we computed for each time instant the matrix E and the error probability P_E, finally averaging over time. The results are reported in Fig. 10, showing the QBER due to compensation error as a function of λ_P. Perfect compensation is clearly possible using a wavelength for the probe beam very close to that of the signal beam. However an acceptable error rate (below one percent), is possible for wavelengths much more distant than our signal one.

3.2. Time-multiplexing of signal and probe beam

A different compensation scheme can be time-multiplexing of signal and probe pulses at the same wavelength in the channel. In this case, suppose to send the probe pulses with repetition rate f_P, so that the m-th probe pulse will be emitted at time $t_m^{(0)} = mT_0$ with $T_0 = 1/f_P$. Between any two probe pulses, N single-photon pulses will be transmitted, each at the time $t_{m,i} = t_m^{(0)} + i\delta$ where $\delta = T_0/N$. In other words, we measure the channel Jones matrix $C(t_m^{(0)})$ and use it to compensate N subsequent single-photon pulses:

$$J\left[t_m^{(0)} + i\delta\right] = C^{-1}(t_m^{(0)}) J_0\left[t_m^{(0)} + i\delta\right] \tag{27}$$

The repetition rate of such pulses must be fast enough to characterize in real-time the evolution of the channel properties. Assuming that this is the case, the amount of change for a Stokes parameter $S_j(t)$ at a time Δt slightly after $t_m^{(0)}$ is small and can be expressed with a Taylor expansion to the first order:

$$S_j(t_m^{(0)} + \Delta t) - S_j(t_m^{(0)}) \approx \frac{dS_j}{dt}|_{t=t_m^{(0)}} \Delta t \tag{28}$$

If we want to keep the error on $\Delta S_j(t)$ under a certain value ΔS_{max}, the repetition rate of the probing pulses must be:

$$f_P \geq \frac{1}{\Delta S_{max}} \frac{dS}{dt}|_{max} \tag{29}$$

Assuming a maximum value for the time-derivative of the Stokes parameters of 0.02 (see Fig. 11), and stating for the maximum acceptable error on the Stokes parameters $\Delta S_{max} = 10^{-5}$, we get a value of $f_P = 2$ KHz for the probe repetition rate. This value is a large bound on the error, since $|dS/dt|$ is in general much smaller than the maximum value we took.

To have a statistical evaluation of the average error probability we performed some simulations similar to what we did for the different-wavelengths scheme. In this case we computed the probability error as a function of the repetition rate of the probe pulses. The results are shown in Fig. 12.

4. Discussion

In this Section we will analyze the possibility of establishing a quantum key distribution link in different configurations employing a LEO satellite and an optical ground station, for different protocols. Throughout the whole Section, formulas for key-generation rate in the asymptotic limit of a long key will be employed. This is clearly not true for

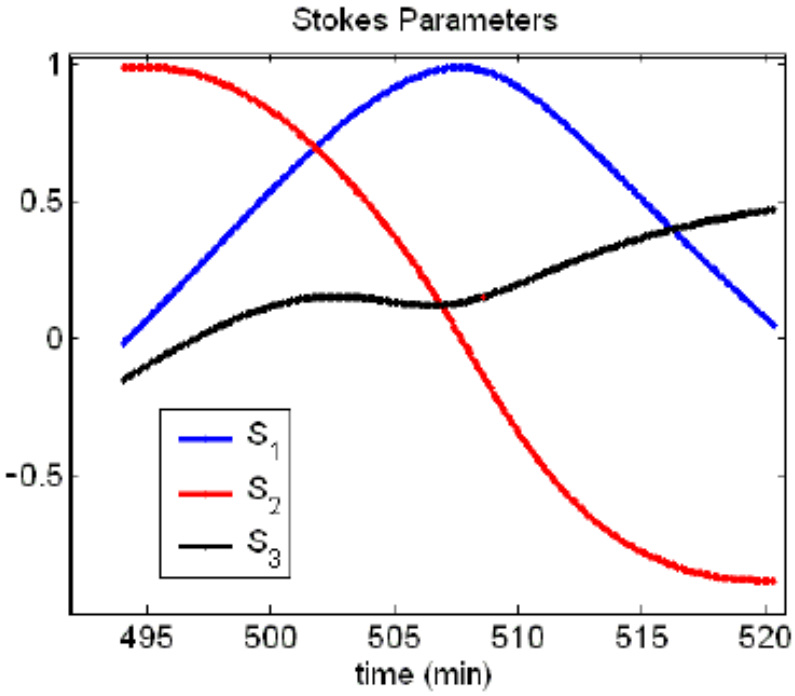


Figure 11. Statistics of the time-derivative of the Stokes parameter S_2 for 1000 passages of two satellites with different orbits (500 Km for the picture on the left, 5000 Km for the one on the right). The temporal evolution of the transformation is faster for the lower-orbit satellite (the absolute value of the time derivative is within 0.015 s^{-1}). For higher satellite the transformation is slower (within 0.005 s^{-1} for the figure on the right)

real-world QKD experiments, especially in the cases involving the exchange of a secret key between a LEO satellite and Earth. At present, the analysis of the security of quantum key distribution for finite key lengths is still an open question [ref] in quantum information theory.

4.1. BB84

The secret key rate per pulse for the BB84 protocol in the case of an ideal single-photon source:

$$R_{BB84}^{(ideal)} \geq \frac{p_{exp}}{2}\left[1 - f(e)H_2(e) - H_2\left(e\right)\right] \tag{30}$$

where p_{exp} is the probability that a non-empty pulse is detected by Bob, e is the QBER, $f(e)$ is the efficiency of error correction and $H_2(x)$ is the binary entropy function: $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$. The efficiency of the classical error correction algorithm is described by the factor $f(e)$: we take $f(e) \approx 1.22$.

In most pratical quantum communication experiments, single photons are implemented with weak coherent pulses, for which there is a non-zero probability to produce multiphoton states. On such multiphoton pulses Eve could perform a photon-

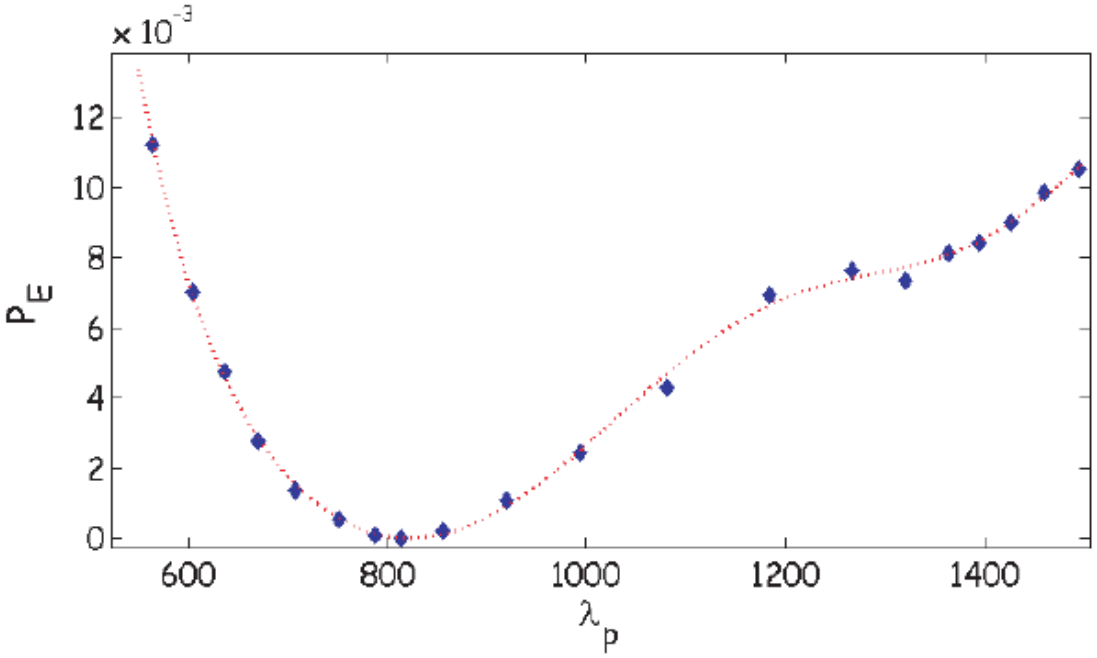


Figure 12. Simulated quantum bit error rate due to imperfect polarization-compensation in the case of a temporal-multiplexing scheme, as a function of the channel-characterization pulses repetition rate. Data are shown for satellites at different altitudes.

number-splitting (PNS) attack [25, 26, 27]. She can split a photon from the multiphoton pulse, store it and measure it in the correct basis after Alice and Bob have pubblicly announced their bases. If she sends the rest of the multiphoton pulse to Bob no noise will be introduce in the channel and she can get complete information about the bit without being discovered. Such bits, that have leaked information to the eavesdropper, are called tagged bits. Inamory et al. [28] and Gottesmann et al. [29] showed that in this situation a secure key can still be distilled and the key generation rate is given by:

$$R_{BB84} \geq \frac{p_{exp}}{2}\left[(1-\Delta) - f(e)H_2(e) - (1-\Delta)H_2\left(\frac{e}{1-\Delta}\right)\right] \tag{31}$$

In the case of an uplink to a LEO satellite the channel is extremely lossy and almost all the single-photon pulses may be wasted, resulting in basically only multiphoton pulses giving clicks in Bob's detectors. Therefore, increasing the channel losses, the fraction of secure bits decreases. If the losses are so strong that only multiphoton pulses are detectd by Bob, no secure key can be generated.

As a worst-case estimate of the fraction of tagged bits Δ we can take the fraction of multiphoton pulses over the fraction on non-empty pulses detected by Bob [26]:

$$\Delta \approx \frac{1 - e^{-\mu} - \mu e^{-\mu}}{1 - e^{-\eta\mu}} \tag{32}$$

In general, given a link attenuation η the key generation rate is of the order of $O(\eta^2)$ (see [30]).

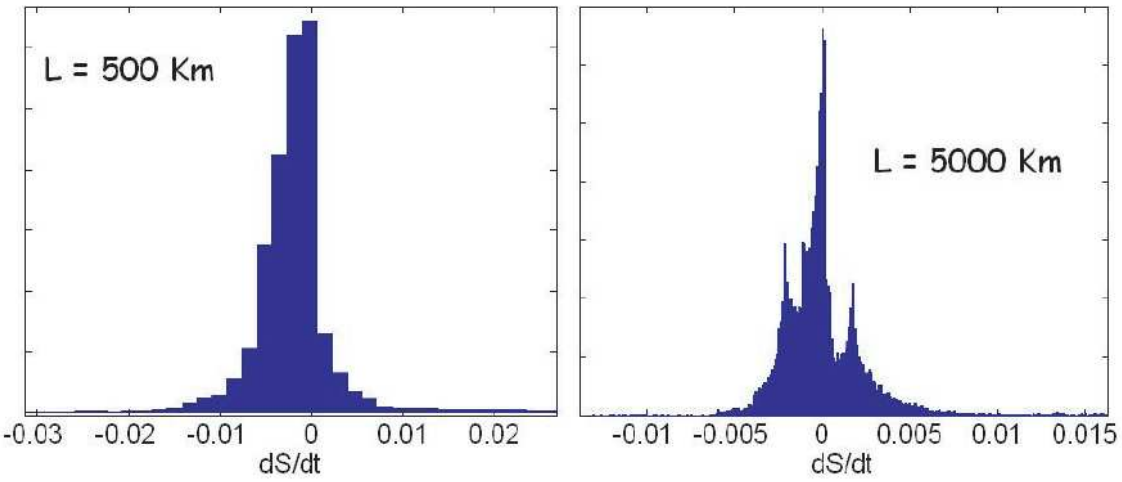


Figure 13. Key-generation rate for the BB84 protocol using weak laser pulses as an approximate single-photon source. On the left side, results for the up-link, in the right side results for the downlink. For the uplink, the channel attenuation is so high that a QKD session with significant key generation rates cannot be implemented, while for the downlinka key-generation rate of 10^{-4} for a satellite orbiting at around 500 km can be obtained using a source with mean photon number $\mu = 0.01$.

Simulations for the key-generation rate as a function of the link distance are shown in Fig. 13. In the case of the uplink the attenuation is so high that the secure key generation rate is extremely low (of the order of 10^{-12}), on the other hand it is not possible to increase the value of μ in order to avoid PNS attacks.

For the downlink, on the contrary, a successful establishment of a BB84 QKD link is possible. Assuming $\mu = 0.01$ (see Fig. 13) and a source repetition rate of 10 MHz, for a satellite at 500-600 km we can get around 1 kbit of secure key per second.

4.2. Decoy-state

To improve the performance of coherent-state weak-pulse QKD, the decoy state method has been proposed [31, 32, 33]. For BB84 protocol, the security analysis is performed using a worst-case estimate on the fraction of bits that are known to the eavesdropper. The decoy-state technique, on the other hand, exploits states with different light intensities to probe the channel transmissivity and error probability, giving a more accurate bound on the amount of tagged bits.

Suppose to use a three-state decoy technique, which exploits vacuum states and two coherent states with mean photon number μ and μ'. Let S_{mu} be Bob's counting rate when Alice transmits pulses with mean photon number μ and S_0 be Bob's counting rate in the case of vacuum-state transmission (therefore due to dark counts and background noise). The bound for Δ is [30]:

$$\Delta \leq \frac{\mu}{\mu' - \mu}\left(\frac{\mu e^{-\mu} S_{\mu'}}{\mu' e^{-\mu'} S_{\mu}} - 1\right) + \frac{\mu e^{-\mu} S_0}{\mu' S_{\mu}} \tag{33}$$

Probing the channel with different light intensity we can get a more accurate estimate of Δ. Consequently, we can guarantee unconditional security without reducing too much the mean photon number of the pulses.

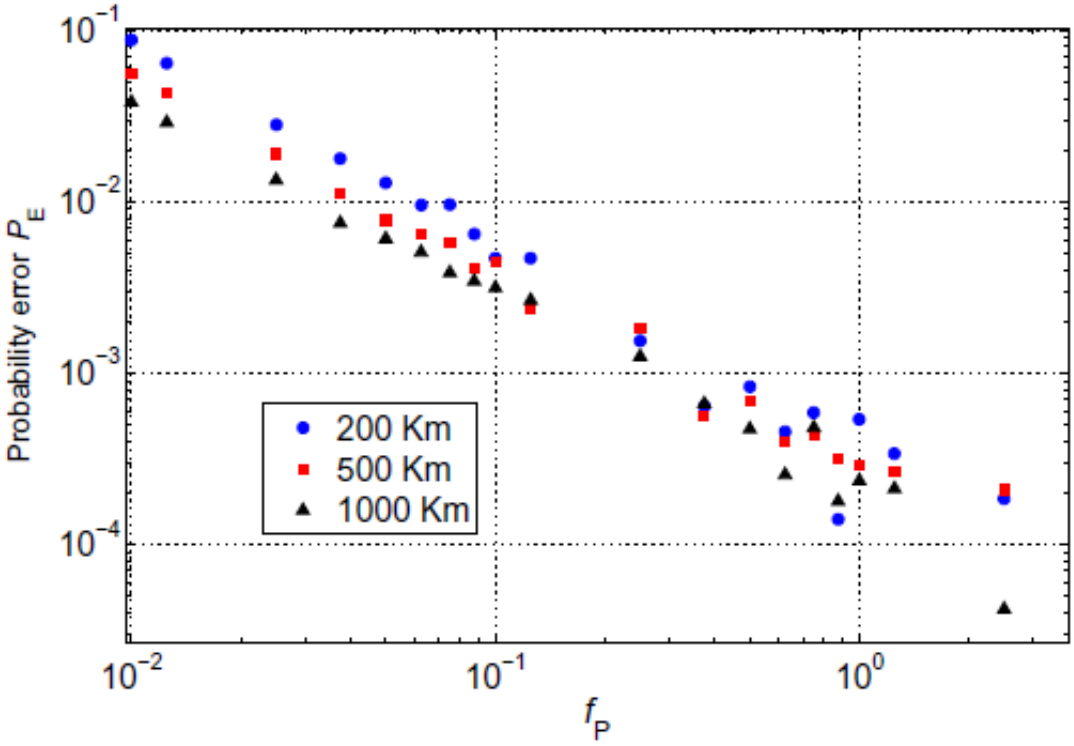


Figure 14. Key-generation rate for the BB84 protocol using a three-level decoy-state protocol (vacuum, $\mu = 0.27$, $\mu' = 0.4$). A secure key rate of 10^{-6} can be obtained for an uplink to satellite orbiting at around 500 km.

In Fig. 14 we show some simulations performed for a three-state decoy method, which employs the vacuum and two coherent-beam intensities $\mu = 0.27$ and $\mu' = 0.4$. Clearly there is a significant improvement in the key-generation rate, from $O(\eta^2)$ to $O(\eta)$. For a source repetition rate of 10 MHz, in the case of an uplink to a satellite at 500 km, we would still be able to get a key generation rate of 10 bits per seconds, as compared to the value of 10^{-5} bits per second one would get for the BB84 protocol with no decoy states.

The main problem in the practical implementation of the decoy-state technique in a a satellite link is the unavoidable intensity fluctuations in such a link due to the fast relative motion of the communication terminals. The situation of decoy-state QKD with intensity fluctuations has been recently analyzed by Xian-Bin Wang in [34], who showed that if the intensity-error of each pulse is random, the decoy-state protocol can work efficiently even in the case of large intensity errors.

4.3. Entangled photons

A detailed analysis of the conditions to violate Bell inequalities and implement a quantum key distribution experiment based on Ekert's protocol has been presented in [19]. As the minimum requirement they assume the SNR needed to violate a Bell-inequality [35]. For the case of polarization-entangled photons this necessitates a coincidence visibility of at least 71 percent, corresponding to a SNR of 6 : 1. Below that ratio it is possible to model the observed correlation with a local realistic theory, allowing unobserved eavesdropping.

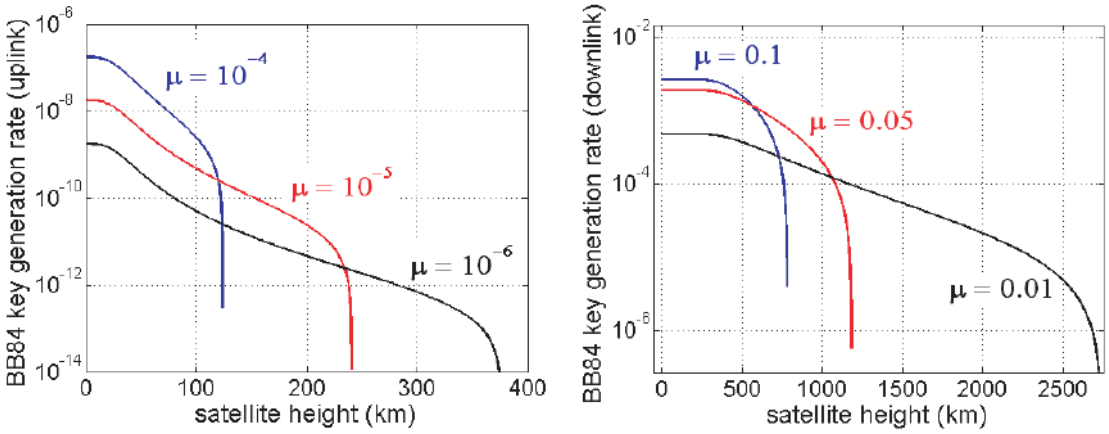


Figure 15. SNR (in dB) for entanglement-based experiments in different configurations.

However, in the analysis they only consider the effect of dark counts, neglecting the effect of background noise. The rate of accidental coincidences is:

$$C_{acc} = N_1 N_2 \Delta t \tag{34}$$

while the rate of good coincidencres is:

$$C = P_0 \eta_1 \eta_2 \tag{35}$$

where η_i is the efficiency of the link i. In our simulations we use the link efficiencies and the noise values calculated in Section 2 for satellite links, while in the case of local detection we use $\eta_i \approx 0.5$ and for the noise counts just the detector dark counts ($N_i \approx 200$ counyts per second). P_0 is the emission rate of the entangled-photon pairs: values of the order of $10^6 - 10^7$ pairs per second are currently available using for examples periodically-poled nonlinear crystals.

We consider four different scenarios:

- source is on the satellite, with two ground receivers (the scheme proposed for the SpaceQUEST experiment [36])
- source on the satellite with one local receiver and the other one on ground
- source on ground, with two satellite-based receivers

- source on ground with one local receiver and the other one on satellite

All simulations were performed for night-time new moon conditions. The results are shown in Fig.15. It is clear that entanglement-based experiments with one photon measured locally at the source and the other one propagating either in the uplink or downlink are feasible, due to sufficient SNR (of the order of 100:1 to 1000:1). On the other hand a ground-based source with two uplinks to satellite is clearly un-feasible. The situation with a source on the satellite and two Earth-based receiving telescope is feasible, but only under some stringent requirements on the experimental parameters (telescope diameter, link distance, filtering...).

5. Conclusions

In this paper we discussed some aspects of the feasibility of satellite-based quantum key distribution which we believe were not yet addressed in the literature.

First of all, we discussed signal propagation through a turbulent atmosphere, refining the models presented in [19], [37]. In particular for the uplink we analyzed the relative contribution of beam spreading and wandering, showing that the former is more important than the latter for low-altitude satellites. This makes the possibility of compensating the beam wandering with an active tip/tilt mirror not worth. Then we introduced a model for the background noise of the channel during night-time and day-time, and we discussed the signal-to-noise ratio for different configurations.

Second, we discussed the polarization properties of a satellite-based quantum channel, discussing two possible compensation techniques to the effects illustrated in [23]. For both techniques (channel-probing at a different wavelength and time-multiplexing of signal and probe pulses at the same wavelength) we showed that the bit error rate can be kept at really low levels.

Finally we discussed the generation rate of a secure key for different configurations and for different protocols. For the standard BB84 protocol (with Poissonian-distributed source) we showed that a QKD link can be established for the downlink with a good generation rate, but not for the uplink. On the other hand, a QKD uplink can be realized with the more accurate estimate of the fraction of bits for which an eavesdropper could have complete information without introducing any disturbance, provide by the decoy-state techniques. Two points are still unclear in our opinion: the effect of the finite duration of the satellite link to the securire key generation and the possibility to implement the decoy-state technique in a channel with strong and random intensity fluctuations. We also discussed the implementation of entanglement-based links, showing that configurations with one photon detected locally at the source and one propagating either in pulink or downlink is feasible with realistic experiemntal parameters. The situation with a source on satellite and two ground-based receivers is also feasile, but with particular care on the choice of the relevant hardware parameters.

In conclusion, we believe that satellite-based quantum key distribution is certainly feasible with present technology. We also believe that Space technology can provide a

rich environment for experiments on foundational quantum mechanics and on quantum-information applications.

6. Acknowledgements

The authors would like to thank dr. Georg Kirchner of the Space Research Center in Graz for assistance with the KHz laser-ranging data. This research was supported by the Italian Space Agency via the Phase A feasbility study SpaceQ and by the research project QUINTET of the Department of Information Engineering, University of Padova.

7. References

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[2] D. Bouwmeester, Artur Ekert, and Anton Zeilinger. *The Physics of Quantum Information*. Springer, 2000.

[3] G. Jaeger. *Quantum Information: an overview*. CSpringer, 2006.

[4] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.

[5] A. V. Sergienko, editor. *Quantum Communication and Cryptography*. CRC, 2005.

[6] Hoi-Kwong Lo and Yi Zhao. Quantum cryptography. arXiv:0803.2507.

[7] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[8] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introductionto Quantum Computing*. Oxford University Press, USA, 2007.

[9] Hiroki Takesue, Sae Woo Nam, Qiang Zhang, Robert H. Hadfield, Toshimori Honjo, Kiyoshi Tamaki, and Yoshihisa Yamamoto. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nat. Phot.*, 1:343–348, 2007.

[10] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement based quantum communication over 144 km. *Nature Physics*, 3:481–486, 2007.

[11] http://www.secoqc.net/.

[12] Cheng-Zhi Peng, Tao Yang, Xiao-Hui Bao, Jun-Zhang, Xian-Min Jin, Fa-Jong Feng, Bin Yang, Jian Yang, Juan Yin, Qian Zhang, Nan Li, Bao-Li Tian, and Jian-Wei Pan. Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. *Phys. Rev. Lett.*, 94:150501, 2005.

[13] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98(1):010504, 2007.

[14] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between space and earth. *New J. Phys.*, 10(033038), 2008.

[15] Ronald Fante. Electromagnetic beam propagation in turbulent media: an update. *Proceedings of the IEEE*, 68:1424–1443, 1980.

[16] L. C. Andrews, R. L. Philips, and P. T. Yu. Optical scintillation and fade statistics for a satellite-communication system. *Appl. Opt.*, 34:7742–775164, 1995.

[17] Federico Dios, Juan Antonio Rubio, Alejandro Rodriguez, and Adolfo Comeron. Scintillation and beam-wander abnalysis in an optical ground station-satellite uplink. *Applied Optics*, 43:3866–3873, 2004.

[18] Masahiro Toyoda. Intensity fluctuations in laser links between ground and a satellite. *Appl. Opt.*, 44:7364, 2005.

[19] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger. Long distance quantum communication with entangled photons using satellites. *IEEE J. Sel. Top. Quantum Electron.*, 9:1541, 2003.

[20] Miao Er-long, Han Zheng-fu, Gong Shun-sheng, Zhang Tao, Diao Da-sheng, and Guo Guang-can. Background noise of satellite-to-ground quantum key distribution. *New J. Phys.*, 7:215, 2005.

[21] R. J. Hughes, J. E. Nordholt, D. Derkacs, and J. C. Peterson. Practical free-space quantum key distribution over 10 km in day-light and at night. *New J. Phys.*, 4:43.1–43.14, 2002.

[22] J. G. Rarity, P. R. Tapster, and P. M. Gorman. Secure free-space key exchange to 1.9 km and beyond. *Journal of Modern Optics*, 48(13):1887–1901, 2001.

[23] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger. Influence of satellite motion on polarization qubits in a space-earth quantum communication link. *Optics Express*, 14(21):10050–10059, 2006.

[24] C. Bonato, C. Pernechele, and P. Villoresi. Influence of all-reflective optical systems in the transmission of polarization-encoded qubits. *J. Opt. A: Pure Appl. Opt.*, 9:899, 2007.

[25] M. Dusek, O. Haderka, and M. Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Opt. Comm.*, 169:103, 1999.

[26] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6), 2000.

[27] Norbert Luetkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.

[28] H. Inamori, N. Luetkenhaus, and D. Mayers. Inconditional security for practical quantum key distribution. *Eur. Phys. J*, 41:599. arXiv:quant-ph/0107017 (2001).

[29] D. Gottesmann, H.-K. Lo, N. Luetkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4(5):325–360, 2004.

[30] Xiang-Bin Wang, Tohya Hiroshima, Akihisa Tomita, and Masahito Hayashi. Quantum information with gaussian states. *Phys. Rep.*, 448:1–111, 2007.

[31] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, Aug 2003.

[32] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

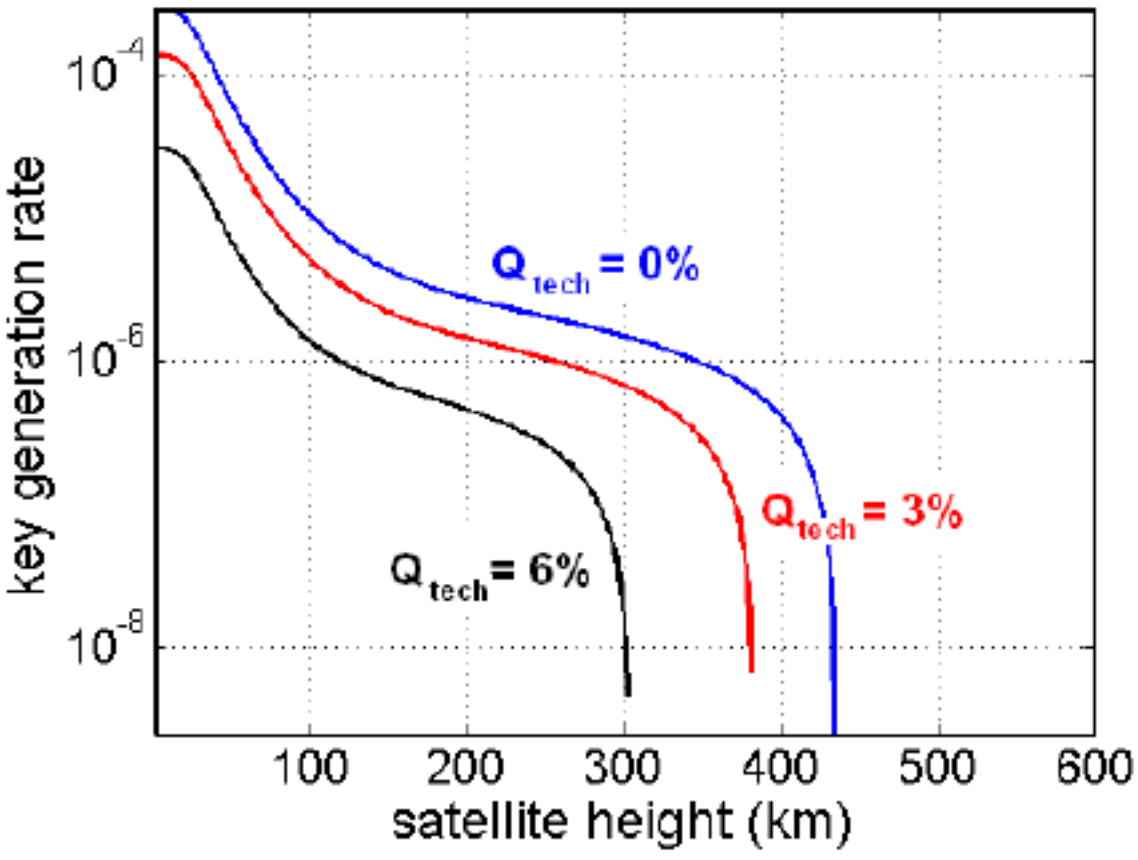
[33] Wang X-B. Beating the photon-number-splitting attack in practical quantum key distribution. *Phys. Rev. Lett.*, 94:230503, 2005.

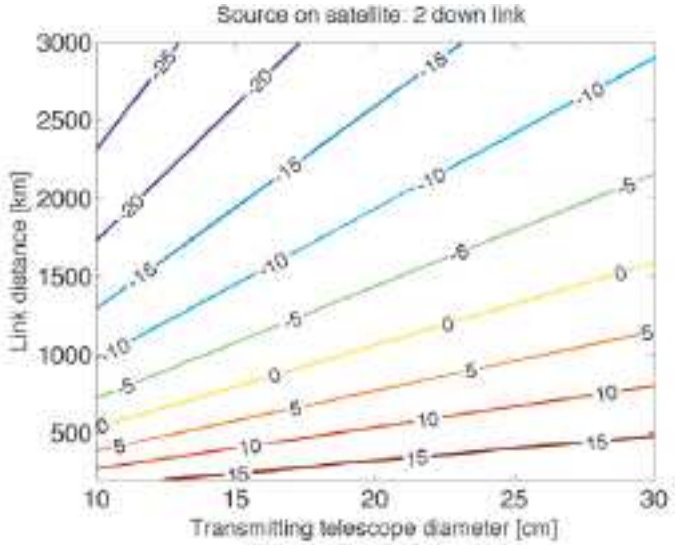
[34] Xiang-Bin Wang. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A*, 75(052301), 2007.

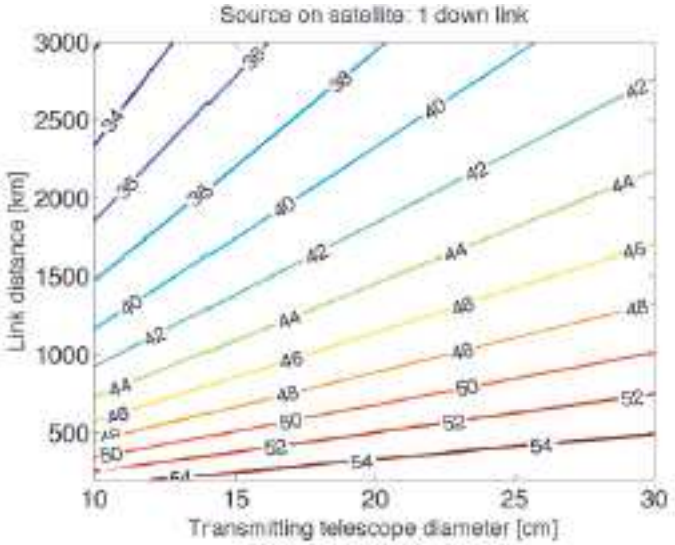
[35] Christopher A. Fuchs, Nicolas Gisin, and Asher Peres Robert B. Griffiths, Chi-Sheng Niu3. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Phys. Rev. A*, 56(2):1163–1172, 1997.

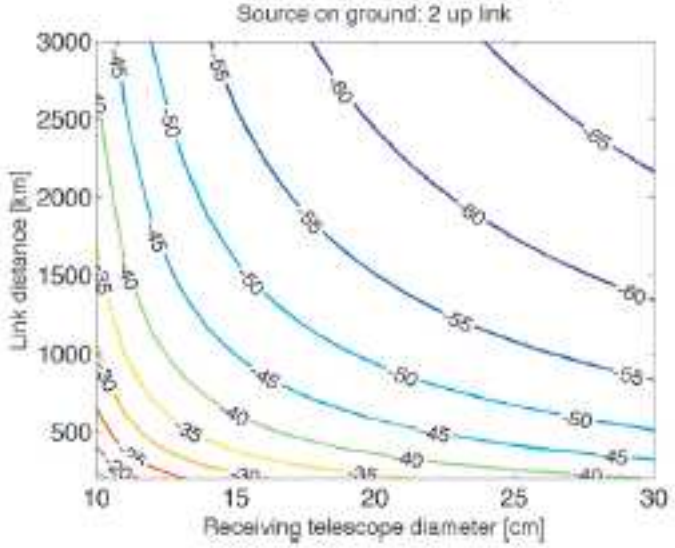
[36] R. Ursin et al. Space-quest: Experiments with quantum entanglement in space. arXiv:0806.0945v1, 2008.

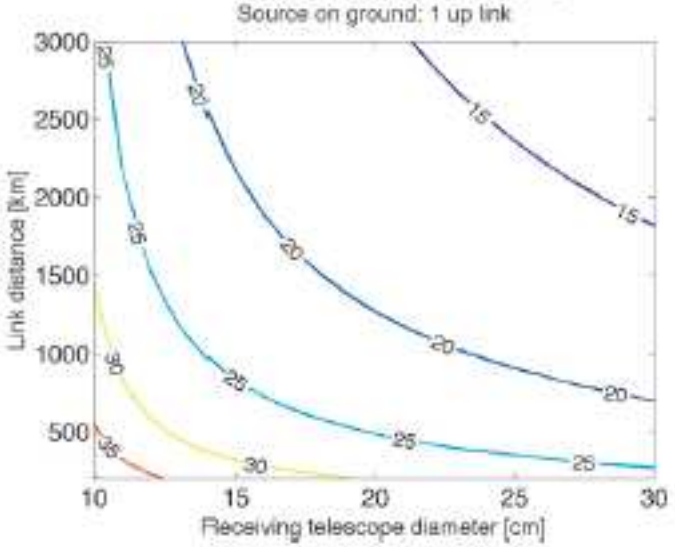
[37] J. G. Rarity, P.R. Tapster, P. M. Gorman, and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.*, 4:82, 2002.


key generation rate
10^-4
10^-6
10^-8
Q_tech = 0%
Q_tech = 3%
Q_tech = 6%
100
200
300
400
500
600
satellite height (km)


Source on satellite: 2 down link
Link distance [km]
Transmitting telescope diameter [cm]


Source on satellite: 1 down link
Link distance [km]
Transmitting telescope diameter [cm]


Source on ground: 2 up link
Link distance [km]
Receiving telescope diameter [cm]


Source on ground: 1 up link
Link distance [km]
Receiving telescope diameter [cm]